Balík nástrojov MS Sysinternals

1st Marek Čederle
Fakulta informatiky a informačných technológií
Slovenská Technická Univerzita v Bratislave
Bratislava, Slovensko
xcederlem@stuba.sk

***Abstrakt*—TODO: WRITE AN ABSTRACT This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***Index Terms*—TODO: INSERT KEYWORDS, component, formatting, style, styling, insert.**

I. Funkčný opis bezpečnostného nástroja

A. Úvod do MS Sysinternals

Windows Sysinternals je webová stránka, ktorá ponúka technické zdroje a nástroje na správu, diagnostiku, riešenie problémov a monitorovanie prostredia Microsoft Windows. Pôvodne bola webová stránka Sysinternals (predtým známa ako ntinternals) vytvorená v roku 1996 a prevádzkovala ju spoločnosť Winternals Software LP[1] so sídlom v Austine v Texase. Založili ju softvéroví vývojári Bryce Cogswell a Mark Russinovich. 18. júla 2006 spoločnosť Winternals a jej aktíva kúpila spoločnosť Microsoft[3].

Webová stránka obsahovala niekoľko freewarových nástrojov na správu a monitorovanie počítačov so systémom Microsoft Windows. Tento softvér teraz nájdete na adrese Microsoft. Spoločnosť predávala aj nástroje na obnovu dát a profesionálne edície svojich freewarových nástrojov.

B. Prehľad Vybraných Nástrojov

1) Process Explorer:

- Čo je Process Explorer?
- Hlavné funkcie: monitorovanie systému, vizualizácia stromu procesov, analýza DLL, atď.

2) AutoRuns:

- Účel nástroja AutoRuns: správa programov spúšťaných pri štarte systému.
- Kľúčové funkcie: identifikácia programov pri štarte, overenie podpísaných súborov, kontrola naplánovaných úloh.

3) TCPView:

- Úloha pri monitorovaní sieťovej aktivity.
- Funkcie: zobrazenie sieťových pripojení, riešenie DNS, monitorovanie TCP/UDP prevádzky.

4) Process Monitor:

- Čo robí: monitorovanie súborového systému, registrov a procesov v reálnom čase.
- Zaujímavé funkcie: filtrovanie udalostí, sledovanie systémových volaní, hľadanie neoprávnených zmien.

C. Porovnanie s Inými Bezpečnostnými Nástrojmi

Ako sa nástroje Sysinternals porovnávajú s inými populárnymi bezpečnostnými balíkmi (napr. Process Hacker, Wireshark, GlassWire)? Výhody a nevýhody.

II. Požiadavky na inštaláciu a postup pri inštalácii

A. Systémové Požiadavky

- Podporované operačné systémy.
- Hardvérové požiadavky (ak nejaké sú).
- Predpoklady (napr. používateľské oprávnenia, práva správcu).

B. Inštalačný Proces

1) Sťahovanie Nástrojov:

- Kde sťahovať jednotlivé nástroje (oficiálna stránka Microsoftu Sysinternals).
- Formáty súborov (ZIP, EXE, atď.) a veľkosť.

2) Inštalácia/Spustenie:

- Krok za krokom návod na spustenie a inštaláciu jednotlivých nástrojov.
- Vysvetlenie samostatných nástrojov (netreba inštalovať, len spustiť).
- Rozdiely medzi spúšťaním nástrojov lokálne a zo sieťového zdieľania.

C. Konfigurácia po Inštalácii

- Úvodné nastavenia a konfigurácie pre jednotlivé nástroje.
- Nastavenie prostredia pre monitorovanie a diagnostiku.

III. Experimentovanie a overeniu základných funkcionalít bezpečnostného nástroja

A. Príprava na Experimentovanie

- Prehľad [1] testovacieho prostredia: verzia OS, virtuálny stroj (ak sa použil), základná konfigurácia.
- Popis scenára alebo prípadu použitia: príklady scenárov pre testovanie každého nástroja.

B. Experimenty s Konkrétnymi Nástrojmi

1) Process Explorer:

- Analýza bežiacich procesov a identifikácia anomálií.
- Použitie vyhľadávacích funkcií na sledovanie konkrétnych súborov alebo procesov.
- Experimentovanie s integráciou ”VirusTotal”.

2) AutoRuns:

- Zoznam všetkých programov a služieb spúšťaných pri štarte.
- Povolenie/zablokovanie položiek a kontrola vplyvu na správanie systému.
- Overovanie digitálnych podpisov spúšťacích položiek.

3) TCPView:

- Monitorovanie živých sieťových pripojení.
- Identifikácia nezvyčajných vzdialených pripojení.
- Analýza stavov pripojenia (napr. TIME_WAIT, LISTENING).

4) Process Monitor:

- Filtrovanie konkrétnych registrov, súborového systému alebo sieťových udalostí.
- Vytváranie filtrov udalostí na zachytenie cieľových aktivít.
- Identifikácia zmien v registroch alebo súboroch počas inštalácií softvéru.

IV. Dokumentovanie experimentovania s nástrojom formou napríklad riadacich príkazov alebo obrazoviek alebo nastavení

A. Podrobné Správy z Experimentov

- Screenshoty zobrazujúce kroky a výsledky každého experimentu.
- Príklady príkazov alebo konfigurácií použitých v experimentoch.

B. Analýza Záznamov a Výstupov

- Prezentácia záznamov alebo dát zhromaždených pomocou každého nástroja.
- Ako interpretovať zhromaždené informácie.
- Porovnanie očakávaných a pozorovaných výsledkov.

C. Problémy, na ktoré sa Narazilo, a Riešenia

- Dokumentovanie akýchkoľvek problémov alebo chýb počas experimentov.
- Kroky na vyriešenie problémov alebo úpravu nastavení.

V. Hodnotenie bezpečnostného nástroja

A. Účinnosť a Spoľahlivosť

Ako dobre si nástroje viedli vo vašich experimentoch? Zaznamenané silné stránky alebo slabiny.

B. Jednoduchosť Použitia a Užívateľské Rozhranie

Ako intuitívne sú rozhrania pre jednotlivé nástroje? Prístupnosť pre začiatočníkov a pokročilých používateľov.

C. Vplyv na Výkon

Vplyv spustenia nástrojov na výkon systému. Zaznamenané spomalenia alebo špičky vo využití zdrojov.

D. Bezpečnosť a Presnosť

Presnosť pri identifikácii procesov, sieťovej aktivity, programov pri štarte. Hodnotenie bezpečnostných funkcií.

E. Návrhy na Vylepšenie

- Odporúčané zmeny alebo doplnky pre budúce verzie.
- Nápady na integráciu s inými nástrojmi alebo funkciami.

LITERATÚRA

[1] Scott Lott, “Installing Windows on a Linode VPS,” 2023, accessed: 2024-10-26. [Online]. Available: https://github.com/only-cliches/docs/blob/windows-on-linode/docs/tools-reference/windows-on-linode/installing-windows-on-linode-vps.md